UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

| | |
|---|---|
| LEAH WALLACE, STEVEN SUPER, STEPHEN GYSCEK, ALEXYS WILLIAMSON, NICOLE DIGILIO, and CHUNG SUK CRISPELL, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>HEALTH QUEST SYSTEMS, INC.,<br><br>Defendant. | **OPINION AND ORDER**<br><br>20 CV 545 (VB) |

Briccetti, J.:

Plaintiffs Leah Wallace, Steven Super, Stephen Gyscek, Alexys Williamson, Nicole Digilio, and Chung Suk Crispell bring this putative class action against Health Quest Systems, Inc. ("Health Quest"), alleging claims for (i) negligence, (ii) breach of implied contract, (iii) breach of contract, (iv) unjust enrichment, (v) breach of confidence, (vi) bailment, (vii) violations of Section 349 of New York's General Business Law ("GBL"), and (viii) violations of GBL § 899-aa. Plaintiffs' claims arise out of a data breach whereby unknown individuals allegedly accessed plaintiffs' sensitive information, including medical records and Social Security numbers.

Now pending is defendant's motion to dismiss the amended complaint pursuant to Rules 12(b)(1) and 12(b)(6). (Doc. #42).

For the reasons set forth below, the motion is GRANTED IN PART and DENIED IN PART.

Plaintiffs allege the Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2).[1]

**BACKGROUND**

For the purpose of ruling on the motion to dismiss, the Court accepts as true all well-pleaded factual allegations in the amended complaint and draws all reasonable inferences in plaintiffs' favor, as set forth below.

Health Quest is a not-for-profit corporation that operates a group of hospitals and healthcare providers in New York and Connecticut. Plaintiffs allege they were all customers or patients of Health Quest's facilities and healthcare providers.

I. The Data Breach

Plaintiffs allege Health Quest learned of a "phishing" incident in July 2018 (the "Data Breach").[2] (Doc. #34 ("AC") ¶ 2). Defendant allegedly learned an unauthorized party gained access to the emails and attachments of certain Health Quest employees. According to plaintiffs, these emails and attachments may have contained certain patients' sensitive personal data, including: patient names, dates of birth, Social Security numbers, driver's license numbers, financial account information, PIN numbers and security codes, payment card information, the

[1] The Class Action Fairness Act ("CAFA") confers federal jurisdiction over certain class actions with an amount in controversy of at least $5 million, when the class exceeds 100 individuals, and the parties are minimally diverse. 28 U.S.C. § 1332(d). Because the Court presumes the amended complaint is a good faith representation of the amount in controversy, and because defendant does not argue there is a legal certainty that the amount recoverable is less than $5 million, the Court resolves any doubt in favor of plaintiffs and finds subject matter jurisdiction under CAFA is adequately alleged at this stage of the case. See Chase Manhattan Bank, N.A. v. Am. Nat. Bank & Tr. Co. of Chicago, 93 F.3d 1064, 1070 (2d Cir. 1996).

[2] "Phishing" refers to "a scam by which an Internet user is duped (as by a deceptive email message) into revealing personal or confidential information which the scammer can use illicitly." Phishing, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/phishing (last visited Mar. 20, 2021).

names of their healthcare providers, dates of treatment, diagnosis information, and health insurance claims information (the "Private Information"). Plaintiffs claim the Private Information of 28,910 patients was potentially compromised and disclosed to cybercriminals.

Health Quest hired an external cybersecurity firm to investigate the Data Breach. Plaintiffs allege this investigation concluded in April 2019, but Health Quest failed to notify its customers that their Private Information had been compromised until late May or early June 2019.

On May 31, 2019, Health Quest posted a notice to its website announcing it had learned of the Data Breach. This notice informed plaintiffs that certain Private Information had been compromised. Defendant also mailed letters containing substantially the same information to patients and customers who were potentially impacted by the Data Breach.

Subsequently, in January 2020, defendant posted a notice on its website stating: "Health Quest is committed to protecting the confidentiality and security of our patients' and employees' information," and defendant had "determined some patient information may have been contained in an email account, accessed by an unauthorized party." (AC ¶ 37). Plaintiffs allege defendant posted this notice after conducting a second investigation of the Data Breach and discovering that both additional Private Information had been compromised and more patients were affected than defendant acknowledged in May 2019.

In its January 2020 website notice, defendant stated it had "determined emails and attachments in some employees' email accounts contained information pertaining to current and former patients and employees," and although the information varied by individual, it included "names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment,

treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims information, financial account information with PIN/security code, and payment card information." (AC ¶ 37).

Plaintiffs allege defendant mailed them a letter dated January 3, 2020 (the "Notice Letter"). (AC ¶ 38). The letter stated Health Quest was "committed to protecting the confidentiality and security of [its] patients information," that it determined plaintiffs' Private Information may have been compromised through the Data Breach, and recommended plaintiffs "regularly review the statements that [they] receive from [their] healthcare insurers and providers." (Id.) Defendant was allegedly "taking steps to help prevent a similar incident from occurring in the future, including the implementation of multi-factor authentication for email, as well as additional procedures to strengthen and expand [its] security processes." (Id.). And defendant also claims it was "providing additional training to [its] employees regarding phishing emails and other cybersecurity issues." (Id.).

II. Defendant's Privacy Practices and Alleged Obligations

Plaintiffs allege defendant maintained a "Notice of Privacy Practices" from 2014 through the date of the Data Breach. (AC ¶ 46). The Notice, which is available on Health Quest's website, states in a section titled "PLEDGE REGARDING MEDICAL INFORMATION" that Health Quest "understand[s] that medical information about you and your health is personal. We are committed to protecting medical information about you." (AC ¶ 46 n.2). Defendant further states it would notify customers in writing if it discovered a breach of customer health information unless it determined it was not obligated to do so by law.

Plaintiffs further allege defendant had certain obligations to ensure the security of their Private Information under regulations implementing the Health Insurance Portability and

Accountability Act ("HIPAA"). See, e.g., 45 C.F.R. § 164.306. For example, plaintiffs claim defendant was required to protect against reasonably anticipated threats or hazards to the security or integrity of electronic private health information, ensure the confidentiality and integrity of electronic protected health information, and train all members of its workforce on policies and procedures regarding private health information.

Additionally, plaintiffs allege their Private Information could be sold for up to $90 on "the black market." (AC ¶ 69). They also claim several government publications and highly publicized incidents made defendant aware, or should reasonably have made it aware, that their Private Information was highly sensitive and could be used for illicit purposes by cybercriminals if disclosed.

Plaintiffs allege Health Quest enabled the Data Breach by failing to abide by industry standards and best practices. For example, plaintiffs claim defendant should have implemented multi-factor authentication, appropriate training, and data encryption to protect their Private Information.

III. Plaintiffs and Their Alleged Damages

Plaintiffs bring this action on behalf of themselves and other similarly situated Health Quest patients and customers who they allege were harmed by the Data Breach.

Plaintiffs all allege they spent time and energy responding to the Data Breach in some fashion. For example, plaintiff Wallace alleges she spent an hour online purchasing credit monitoring services and has spent several hours calling her doctors and attempting to ascertain whether her Private Information was compromised. And plaintiff Gyscek claims he spent several hours attempting to reach Health Quest's helpline to better understand the nature of the Data Breach and how he could protect himself.

Each plaintiff also claims he or she is at a continuing risk of future injury as a result of the Data Breach because they are more likely to be the victims of identity theft. In addition, each plaintiff claims their Private Information diminished in value as a result of the Data Breach.

Plaintiffs Wallace, Super, Williamson, and Crispell all claim they purchased and enrolled in identity protection and credit monitoring services in response to the Data Breach. Plaintiffs Digilio and Gyscek do not allege they purchased credit monitoring services.

Three plaintiffs say they were victims of attempted fraud. Wallace claims she was "denied access to her debit card several times following her receipt of the Notice Letter because the card had been flagged for fraud." (AC ¶ 14). Super claims that, after receiving notice of the Data Breach, he was contacted by a medical provider he never used who attempted to confirm an appointment he never made. Similarly, Gyscek claims he received a text message alerting him a security code was needed to complete a credit application initiated in his name, but that he never initiated that application.

Finally, plaintiffs claim they were denied the benefit of the bargain for Health Quest's services because they paid for those services expecting they included adequate data security. But plaintiffs allege Health Quest did not "properly comply with their data security obligations" and so plaintiffs "did not get what they paid for." (AC ¶ 55). They also allege that, had they known Health Quest did not adequately protect their Private Information, they would not have purchased services from Health Quest.

## DISCUSSION

I. Standards of Review

A. Rule 12(b)(1)

"[F]ederal courts are courts of limited jurisdiction and lack the power to disregard such limits as have been imposed by the Constitution or Congress." Durant, Nichols, Houston, Hodgson & Cortese-Costa, P.C. v. Dupont, 565 F.3d 56, 62 (2d Cir. 2009).[3] "A case is properly dismissed for lack of subject matter jurisdiction under Rule 12(b)(1) when the district court lacks the statutory or constitutional power to adjudicate it." Nike, Inc. v. Already, LLC, 663 F.3d 89, 94 (2d Cir. 2011). A court lacks the power to hear a party's claims when the party does not have standing. Hillside Metro Assocs., LLC v. JPMorgan Chase Bank, Nat'l Ass'n, 747 F.3d 44, 48 (2d Cir. 2014). "When the Rule 12(b)(1) motion is facial, i.e., based solely on the allegations of the complaint . . ., the plaintiff has no evidentiary burden," and "[t]he task of the district court is to determine whether the [complaint] alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue." Carter v. HealthPort Techs., LLC, 822 F.3d 47, 56 (2d Cir. 2016).

When deciding whether subject matter jurisdiction exists at the pleading stage, the court "must accept as true all material facts alleged in the complaint." Conyers v. Rossides, 558 F.3d 137, 143 (2d Cir. 2009). "However, argumentative inferences favorable to the party asserting jurisdiction should not be drawn." Buday v. N.Y. Yankees P'ship, 486 F. App'x 894, 895 (2d Cir. 2012) (summary order).

[3] Unless otherwise indicated, case quotations omit all internal citations, quotations, footnotes, and alterations.

When a defendant moves to dismiss for lack of subject matter jurisdiction and on other grounds, the court should resolve the Rule 12(b)(1) challenge first. Rhulen Agency, Inc. v. Ala. Ins. Guar. Ass'n, 896 F.2d 674, 678 (2d Cir. 1990).

B. Rule 12(b)(6)

In deciding a Rule 12(b)(6) motion, the Court evaluates the sufficiency of the complaint under the "two-pronged approach" articulated by the Supreme Court in Ashcroft v. Iqbal, 556 U.S. 662, 679 (2009). First, plaintiff's legal conclusions and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements," are not entitled to the assumption of truth and thus are not sufficient to withstand a motion to dismiss. Id. at 678; Hayden v. Paterson, 594 F.3d 150, 161 (2d Cir. 2010). Second, "[w]hen there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." Ashcroft v. Iqbal, 556 U.S. at 679.

To survive a Rule 12(b)(6) motion, the complaint's allegations must meet a standard of "plausibility." Ashcroft v. Iqbal, 556 U.S. at 678; Bell Atl. Corp. v. Twombly, 550 U.S. 544, 564 (2007). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. at 678. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." Id. (quoting Bell Atl. Corp. v. Twombly, 550 U.S. at 556).

II. Standing

Defendant argues plaintiffs do not allege an injury-in-fact sufficient to support Article III standing.

The Court disagrees.

To satisfy the "irreducible constitutional minimum of standing . . . the plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016). "The task of the district court" in deciding a motion to dismiss for lack of standing "is to determine whether the [complaint] alleges facts that affirmatively and plausibly suggest that the plaintiff has standing to sue." Id.

An injury-in-fact is "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." Spokeo, Inc. v. Robins, 136 S. Ct. at 1548. "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes." Clapper v. Amnesty Intern. USA, 568 U.S. 398, 409 (2013). An allegation of a threatened injury in the future is sufficient to establish standing "if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014).

Satisfying the injury-in-fact requirement is "a low threshold which helps to ensure that the plaintiff has a personal stake in the outcome of the controversy." John v. Whole Foods Mkt. Grp., Inc., 858 F.3d 732, 736 (2d Cir. 2017). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support a claim." Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992).

Other courts have found the imminent risk of identity theft sufficient to satisfy Article III's injury-in-fact requirement. See, e.g., Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d 739, 746 (S.D.N.Y. 2017) (finding plaintiffs alleged an imminent risk of identity theft sufficient

to satisfy Article III when plaintiffs personal information was disclosed in data breach); Galaria v. Nationwide Mutual Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (finding allegations of "a substantial risk of harm, coupled with reasonably incurred mitigation costs" sufficient to allege an Article III injury).

Plaintiffs adequately allege injury-in-fact here. They allege their sensitive Private Information was accessed by unknown third parties and they are thereby exposed to a high degree of risk of identity fraud and future economic harm. (See, e.g., AC ¶¶ 1–8, 35–41). Given the potential wealth of information compromised, plaintiffs suffer a substantial risk that harm will occur to their reputations, their identities, their financial accounts, and more at the hands of the unknown hackers who accessed defendant's systems. At a minimum, plaintiffs have alleged an imminent risk of future identity theft and fraud.

Accordingly, plaintiffs sufficiently plead Article III standing.

III. Damages

Defendant next argues plaintiffs do not plead they suffered cognizable damages resulting from the Data Breach. Because damages are an element of each of plaintiffs' claims, defendant argues the complaint must be dismissed in its entirety.

The Court again disagrees.

Pleading damages to support a cause of action is distinct from pleading injury-in-fact to support standing. See Doe v. Chao, 540 U.S. 614, 624–25 (2004). Thus, although plaintiffs' allegations are sufficient to support standing, plaintiffs must also plead cognizable damages to survive defendant's motion to dismiss under Rule 12(b)(6).

Plaintiffs bring causes of action sounding in tort and contract, and under New York's consumer protection laws. They assert several theories of damages to support their claims: (i)

being deprived of the benefit of the bargain for services purchased from Health Quest; (ii) costs incurred for purchasing credit monitoring services; (iii) damages caused by attempted fraud; (iv) loss of time spent monitoring their credit and remedying attempted fraud; (v) an imminent threat of future harm through fraud; and (vi) that the value of their Private Information diminished as a result of the Data Breach.

The Court addresses each theory in turn, and concludes plaintiffs plausibly allege cognizable damages by claiming they were deprived of the benefit of the bargain for services they purchased from Health Quest, and incurred out-of-pocket costs purchasing credit monitoring services. These allegations are sufficient to plead cognizable theories of damages for claims sounding in tort and contract, and under New York's consumer protection laws. All plaintiffs plead they were denied the benefit of the bargain for Health Quest's services. However, only plaintiffs Wallace, Super, Williamson, and Crispell allege they incurred out-of-pocket costs sufficient to support claims sounding in tort.

A. Lost Benefit of the Bargain

"Lost benefit of the bargain is a viable theory of injury for breach of contract and unfair competition." Svenson v. Google, Inc., 2015 WL 1503429, at *11 (N.D. Cal. Apr. 1, 2015) ("Svenson I") (allegations that buyer of phone application contracted to keep her information private from third parties were sufficient to allege damages for breach of contract); see also Orlander v. Staples, Inc., 802 F.3d 289, 299–302 (2d Cir. 2015) (finding allegations that plaintiff purchased repair services and did not receive full value sufficient to allege damages for contract and GBL § 349 claims).

Here, all six plaintiffs plausibly plead that "[p]art of the price [they] paid to [d]efendant was intended to be used . . . to fund adequate data security, but was not," and thus plaintiffs "did

not get what they paid for." (AC ¶ 55). Plaintiffs also allege they "provided their Private Information to [d]efendant with the reasonable expectation and mutual understanding that [d]efendant . . . would comply with their obligations to keep [their Private Information] confidential and secure from unauthorized access." (AC ¶ 45). These allegations plausibly allege plaintiffs were denied the benefit of the bargain. See, e.g., In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d at 992–93 (collecting cases on GBL § 349 and finding allegations of lost benefit of the bargain sufficient to allege damages)

Accordingly, plaintiffs plausibly plead they suffered damages cognizable under their claims sounding in contract, and also under New York's consumer protection laws. Orlander v. Staples, Inc., 802 F.3d at 299–300, 301–02 (allegations that plaintiff purchased "carry-in" protection plan for computer but was told he would need to mail computer to manufacturer and therefore lost benefit of the bargain were sufficient to plead restitution damages in contract and under GBL § 349).

B. Costs Incurred Purchasing Credit Monitoring Services

Plaintiffs Wallace, Super, Williamson, and Crispell allege they purchased credit monitoring and identity protection services to reduce the risk of future identity theft from the Data Breach. (AC ¶¶ 12, 16, 24, 26). The Court agrees "[t]hese mitigation expenses satisfy the injury requirements of negligence [and other tort claims]; otherwise [p]laintiffs would face an untenable Catch–22. Under New York's doctrine of avoidable consequences, a plaintiff must minimize damages caused by a defendant's tortious conduct, and can recover mitigation costs for any action reasonable under the circumstances." Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 749 (quotations and alterations omitted).

Accordingly, plaintiffs Wallace, Super, Williamson, and Crispell have plausibly alleged they suffered monetary damages for claims sounding in both tort and contract. See Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 751 (applying the same reasoning to damages for breach of contract claims).

C. Damages Caused by Attempted Fraud

Certain plaintiffs allege they have already been victims of fraud. For example, Super and Gyscek allege their Private Information was accessed to obtain fraudulent medical appointments and credit applications. And Wallace claims she was unable to use her debit card on several occasions because the card was flagged for fraud after the Data Breach.

Plaintiffs argue these allegations sufficiently allege damages.

The Court disagrees.

Plaintiffs do not allege these instances of potential fraud caused any cognizable injuries. Instead, these allegations of damages are inextricably linked to the other theories of damages asserted by plaintiffs. For example, Wallace's inability to use her debit card on certain occasions amounts to no more than an allegation that she needed to expend time and energy re-authorizing its use. Similarly, neither Super nor Gyscek allege the fraudulently scheduled medical appoints or credit applications resulted in any out-of-pocket expenses or monetary loss. Instead, the Court can only infer these instances of potential fraud caused Super and Gyscek to expend time and energy cancelling appointments and cancelling fraudulent credit applications.

Accordingly, plaintiffs do not allege any cognizable damages stemming from instances of potential fraud, alone. No plaintiff alleges his or her bank account was drained of funds or he or she was billed for fraudulently scheduled appointments. Cf., e.g., Cohen v. Northeast Radiology, P.C., 2021 WL 293123, at *2, *6 (S.D.N.Y. Jan. 28, 2021) (plaintiff sufficiently alleged damages

when he was not reimbursed for $10,000 of fraudulent charges to his bank account). Nor does any plaintiff allege reputational or other harm stemming from these instances of potential fraud. And plaintiffs point to no cases supporting the proposition that attempted fraud, alone, is sufficient to support claims for damages.

However, plaintiffs allege these instances of potential fraud caused them to expend time, and in some cases money, to remedy or mitigate against additional fraud or the consequences of potential fraud. Accordingly, the Court addresses those allegations as appropriate.

D. Loss of Time Spent Monitoring Credit and Remedying Attempted Fraud

Each plaintiff alleges he or she spent time responding to the Data Breach by monitoring their credit, responding to potential instances of fraud, or by freezing and unfreezing their credit. They also allege they will need to diligently monitor their credit to avoid future harm.

Such allegations, standing alone, do not plausibly plead cognizable damages. Each of the cases plaintiffs cite for support either involved allegations of lost time and money, or were predicated upon interpretations of unique state statutes. Accordingly, allegations that plaintiffs spent time mitigating or remedying attempted fraud, or monitoring their credit, do not plead cognizable damages.

E. Imminent Threat of Future Harm Through Fraud

Under New York law, a "threat of harm is insufficient to impose liability against a defendant in a tort context." Caronia v. Philip Morris USA, Inc., 22 N.Y.3d 439, 446 (2013).[4] Thus, a plaintiff may only recover damages for a risk of future harm if he or she alleges an

[4] There is no dispute plaintiffs cannot recover in contract for an imminent risk of harm. See Restatement (Second) of Contracts § 347 cmt. e ("The injured party is limited to damages based on his actual loss caused by the breach . . . [and] [r]ecovery can be had only for loss that would not have occurred but for the breach.").

expense is "reasonably certain to be incurred" by virtue of that risk. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008) (quoting Schultz v. Harrison Radiator Div. General Motors Corp., 90 N.Y.2d 311, 321 (1997)).

Plaintiffs do not plausibly allege they are reasonably certain to incur expenses as a result of their greater exposure to fraud and identity theft. Plaintiffs allege their Private Information was accessed by cybercriminals, and according to statistics from governmental agencies, such access could cause lasting harm by costing plaintiffs money, harming their credit scores, and making obtaining loans or other forms of credit difficult. But these allegations raise only the speculative possibility that plaintiffs might, at some point in the future, be victims of fraud and thereby incur monetary or other damages. Accordingly, plaintiffs fall short of alleging expenses that are "reasonably certain to be incurred." See, e.g., Caronia v. Philip Morris USA, Inc., 22 N.Y.3d at 446 (finding plaintiffs failed to allege present damages due to future risk of cancer caused by smoking); Schultz v. Harrison Radiator Div. General Motors Corp., 90 N.Y.2d at 321 (finding error when jury was not instructed to award damages only for household services reasonably certain to be incurred and necessitated by plaintiff's injuries).

Accordingly, allegations that plaintiffs are at risk of future harm are insufficient to plead cognizable damages.

F. Diminished Value of Private Information

Allegations that a plaintiff's private information has lost value may plead a cognizable economic injury. See In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016). However, such allegations are actionable only if the plaintiff also alleges the existence of a market for that information and how the value of such information could have

decreased due to its disclosure. See Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *8 (S.D.N.Y. May 7, 2019).

Plaintiffs do not plausibly allege the Data Breach caused their Private Information to lose value. Plaintiffs allege the existence of a black-market for private information generally. (AC ¶ 69). But plaintiffs provide only speculative allegations regarding the value of their Private Information on that black market and how their Private Information diminished in value. Plaintiffs do not allege they could have monetized their private information, nor do they claim their private information was actually monetized on the black market. Cf. e.g., In re Yahoo! Inc. Customer Data Breach Litig., 2017 WL 727318, at *13–*14 (allegations that information was "highly valuable to identity thieves" and "hackers have sold this [information]," including specific examples of sales, were sufficient to allege plaintiffs lost the value of their private information). They likewise fail to allege that, but for the Data Breach, they could have monetized their own Private Information. See, e.g., Svenson v. Google, Inc., 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016) ("Svenson II") (evidence that plaintiff could not have individually sold her data was sufficient to demonstrate a lack of damages on summary judgment).

Accordingly, plaintiffs do not plausibly allege their Private Information lost value as a result of the Data Breach.

In sum, because plaintiffs plausibly allege damages sufficient to support claims sounding in both tort and contract, and for violations of the GBL, the Court addresses whether plaintiffs plausibly allege their substantive claims.

IV. Negligence

Defendant argues plaintiffs fail plausibly to allege a negligence claim.

The Court disagrees.

A. Applicable Law

Under New York law, to plead a negligence claim, a plaintiff must plausibly allege "(1) the defendant owed the plaintiff a cognizable duty of care; (2) the defendant breached that duty; and (3) the plaintiff suffered damage as a proximate result of that breach." Stagl v. Delta Airlines, Inc., 52 F.3d 463, 467 (2d Cir. 1995).

New York's "economic loss doctrine" precludes recovery in tort for purely economic losses unless the plaintiff alleges "a legal duty independent of [a] contract itself has been violated." Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 749. "This legal duty must spring from circumstances extraneous to, and not constituting elements of, the contract, although it may be connected with and dependent upon the contract." Bristol-Myers Squibb, Indus. Div. v. Delta Star, Inc., 206 A.D.2d 177, 179 (4th Dep't 1994).

B. Application

Plaintiffs (other than Gyscek and Digilio) plausibly plead a claim for negligence. Plaintiffs allege defendant owed them a duty of care to safeguard their Private Information and to not subject their Private Information to an unreasonable risk of exposure and theft. Plaintiffs also allege defendant breached that duty by failing to implement certain safeguards and computer security practices that would have prevented disclosure of their Private Information. According to plaintiffs, defendant's failures directly and proximately caused their Private Information to be exposed to cybercriminals, and thus resulted in plaintiffs incurring out-of-pocket costs.

Defendant argues the economic loss doctrine bars plaintiffs' negligence claim because they allege neither personal injury nor that defendant had a special duty.

The Court disagrees. Plaintiffs allege defendant had duties to safeguard their Private Information separate from any duty that may have been created by a contract. For example, they claim HIPAA implementing regulations required defendant to implement certain safeguards to protect plaintiffs' Private Information. See, e.g., 45 C.F.R. § 164.312 (requiring covered entities to implement "technical policies and procedures for electronic information systems that maintain protected health information to allow access only to those persons or software programs that have been granted access.").

Defendant's arguments are also self-defeating. Not only does defendant argue plaintiffs fail to allege the existence of a contract (which by itself would make the economic loss doctrine inapplicable), but it also acknowledges it has "pre-existing legal duties to" ensure the security of plaintiffs' Private Information. (Doc. #43 ("Def.'s Mem.") at ECF 23–24).[5]

Moreover, as the Court has already concluded, plaintiffs Wallace, Super, Williamson, and Crispell plausibly allege they suffered monetary damages cognizable in tort. However, plaintiffs Gyscek and Digilio fail to plead any monetary losses stemming from the Data Breach. Thus, defendant's motion to dismiss Gyscek and Digilio's claim for negligence must be granted.

In short, plaintiffs plausibly allege a legal duty owed to them by defendant independent of any duty imposed by contract, and the economic loss doctrine does not bar plaintiffs' negligence claim. See Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 749.

V. Breach of Contract

Defendant argues plaintiff alleges neither breach of an express contract nor breach of an implied contract.

[5] Unless otherwise indicated, citations to documents filed on the docket refer to the page numbers automatically assigned by the Court's Electronic Case Filing System, or "ECF."

The Court agrees that plaintiffs do not plausibly allege a claim for breach of an express contract. However, plaintiffs plausibly allege breach of an implied contract.

A. Express Contract

"Under New York law, a breach of contract claim requires proof of (1) an agreement, (2) adequate performance by the plaintiff, (3) breach by the defendant, and (4) damages." Fischer & Mandell, LLP v. Citibank, N.A., 632 F.3d 793, 799 (2d Cir. 2011).

To form a contract "there must be a manifestation of mutual assent sufficiently definite to assure that the parties are truly in agreement with respect to all material terms." Express Indus. & Terminal Corp. v. N.Y. State Dep't of Transp., 93 N.Y.2d 584, 589 (1999). "The first step then is to determine whether there is a sufficiently definite offer such that its unequivocal acceptance will give rise to an enforceable contract." Id. The terms must be "sufficiently certain and specific so that what was promised can be ascertained." Joseph Martin, Jr. Delicatessen v. Schumacher, 52 N.Y.2d 105, 109 (1981).

Plaintiffs do not plausibly allege the "Notice of Privacy Practices" posted on Health Quest's website forms an express contract between Health Quest and its customers. The Notice of Privacy Practices states Health Quest is "committed to protecting medical information," and "will notify you in writing if [it] discover[s] a breach of [plaintiffs'] unsecured health information, unless [it] determine[s], based on a risk assessment, that notification is not required by applicable law." (AC ¶ 46). But these statements do not commit Health Quest to providing a certain level of protection, nor do they obligate Health Quest to institute any particular safeguards. Thus the "terms" of the Notice of Privacy Practices are neither sufficiently certain nor specific enough for the Court to ascertain what—if anything—Health Quest promised.

Plaintiffs allege defendant "specifically promised it 'does not collect any personally identifiable information about you,' other than that specifically disclosed in its policy," and that it would not disseminate "Personal Information through unsecured email." (AC ¶ 126 (alterations omitted)). But these allegations are insufficient. Although plaintiffs cite the Notice of Privacy Practices as the source of this promise, the quoted language appears nowhere in the document. Because plaintiffs fail to allege in detail where, or how, defendant made this promise, the allegation is conclusory and cannot form the basis of plaintiffs' breach of contract claim.

Accordingly, plaintiffs do not plausibly allege the existence of an express contract and their breach of express contract claim must be dismissed.

B. Implied Contract

Under New York law, "[a] contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct." Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc., 448 F.3d 573, 582 (2d Cir. 2006). Contracts implied in fact are "just as binding as an express contract arising from declared intention." Id.

"An implied contract, like an express contract, requires consideration, mutual assent, legal capacity and legal subject matter." Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 751. "The terms of an implied-in-fact contract turn on the conduct of the parties." Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J., Inc., 448 F.3d at 582. And plaintiffs need not plead an implied contract's precise terms to survive a motion to dismiss. See Monahan v. Lewis, 51 A.D.3d 1308, 1310 (3d Dep't 2008).

"A party's conduct indicates assent when 'he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents.'"

Leibowitz v. Cornell Univ., 584 F.3d 487, 507 (2d Cir. 2009) (quoting Restatement (Second) of Contracts § 19(2) (1981)), superseded by statute on other grounds as recognized by Mihalik v. Credit Agricole Cheuvreux N. Am., Inc., 715 F.3d 102, 108–09 (2d Cir. 2013). The existence of "an implied contract will ordinarily be a question of fact, as it involves an assessment of the parties' conduct and the extent to which such conduct demonstrates a meeting of the minds." Monahan v. Lewis, 51 A.D.3d at 1310.

Under New York law, the elements required to allege a breach of implied contract are identical to those necessary to allege a breach of contract. See Forest Park Pictures v. Univ. TV Network, Inc., 683 F.3d 424, 432 (2d Cir. 2012).

Plaintiffs plausibly allege breach of an implied contract here.

The terms of the Notice of Privacy Practices, along with the notices defendant posted on its website, support an inference that Health Quest intended to be bound by its obligation to safeguard plaintiffs' Private Information. Furthermore, that defendant outlines specific security measures it took to prevent further breaches supports an inference that defendant believed it had an obligation to better protect plaintiffs' Private Information.

These facts plausibly allege a course of conduct and dealing that raises an inference of an implied contract for the exercise of reasonable care in protecting plaintiffs' private information in exchange for plaintiffs' provision of business to Health Quest. See, e.g., Sackin v. TransPerfect Global, Inc., 278 F. Supp. 3d at 750–51 (finding implied contract when plaintiffs alleged defendant required them to provide information for employment). Plaintiffs need not plead the implied contract's precise terms to survive a motion to dismiss. See Monahan v. Lewis, 51 A.D.3d at 1310. Furthermore, plaintiffs allege defendant breached this implied contract by failing reasonably to safeguard their Private Information.

Defendant argues plaintiffs cannot plead consideration for an implied contract because Health Quest's alleged obligation to safeguard plaintiffs' Private Information was already required by law.

However, plaintiffs do not allege defendant promised merely to abide by its legal obligations to protect the Private Information under HIPAA. Instead, plaintiffs plausibly allege defendant's promise and commitment to safeguard their Private Information included an obligation to provide security measures beyond those required by HIPAA implementing regulations, such as multi-factor authentication and complex data encryption. Compare AC ¶ 40 (alleging defendant failed to maintain basic security measures such as multi-factor authentication and complex data encryption) with 45 C.F.R. § 164.530(c)(2)(i) ("A covered entity must reasonably safeguard protected health information.").

These allegations are sufficient to allege consideration at the pleading stage. See, e.g., Rudolph v. Hudson's Bay Co., 2019 WL 2023713, at *11 (finding consideration adequately alleged when court could not conclude at pleading stage the extent of overlap between implied promise to maintain data security and California's data protection statute).

Accordingly, plaintiffs plausibly allege a claim for breach of implied contract.

VI. Unjust Enrichment

Defendant argues plaintiffs' claim for unjust enrichment must be dismissed.

The Court disagrees.

To plead unjust enrichment under New York law, "the plaintiff must allege that (1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." Georgia Malone & Co., Inc. v. Reider, 19 N.Y.3d 511, 516 (2012). "The essence of such a claim is that one party

has received money or a benefit at the expense of another." Kaye v. Grossman, 202 F.3d 611, 616 (2d Cir. 2000).

The existence of a contract, whether express or implied, precludes recovery on quasi-contractual claims such as unjust enrichment. Nakamura v. Fujii, 253 A.D.2d 387, 390 (1st Dep't 1998). However, "where a bona fide dispute exists as to the existence of [a] contract, the plaintiff may proceed on both breach of contract and quasi-contract theories." Id.

Plaintiffs plausibly allege a claim for unjust enrichment. They claim they were patients of defendant's healthcare provider network, paid defendant for its services, and were denied those benefits when defendant failed to abide by its obligations to safeguard plaintiffs' Private Information. These allegations plead the "essence" of a claim for unjust enrichment. See Kaye v. Grossman, 202 F.3d at 616.

Furthermore, because defendant disputes whether a contract exists, plaintiffs may proceed with their claims for both breach of implied contract and unjust enrichment. See Nakamura v. Fujii, 253 A.D.2d at 390.

Accordingly, defendant's motion to dismiss plaintiffs' claim for unjust enrichment is denied.

VII. Breach of Confidence

Heath Quest argues plaintiffs fail plausibly to allege defendant is subject to any duty of confidentiality, and therefore plaintiffs' claim for breach of confidence must be dismissed.

The Court disagrees.

A. Legal Standard

Although New York courts have not clearly delineated the elements of a claim for breach of confidence, the sum of cases demonstrates a plaintiff must plead: (i) the defendant assumed a

duty of confidentiality, (ii) the defendant intentionally, knowingly, or negligently breached that duty, and (iii) the plaintiff was damaged as a result of that breach. See Chanko v. Am. Broad. Companies Inc., 27 N.Y.3d 46, 53–54 (2016). For example, at least one New York court has sustained such a claim based on a "fail[ure] to safeguard . . . clients' personal and confidential information." See Daly v. Metro. Life Ins. Co., 4 Misc. 3d 887, 892 (Sup. Ct. N.Y. Cty. 2004).

Although "[b]reach of confidence is a relative newcomer to the tort family," "it has been asserted most frequently in the context of physician-patient" relationships. Young v. United States Dep't of Justice, 882 F.2d 633, 640 (2d Cir. 1989). In fact, the "duty not to disclose confidential personal information springs from the implied covenant of trust and confidence that is inherent in the physician-patient relationship." Doe v. Cmty. Health Plan–Kaiser Corp., 268 A.D.2d 183, 183 (3d Dep't 2000), overruled in part by Doe v. Guthrie Clinic, Ltd., 22 N.Y.3d 480 (2014) (rejecting that strict liability applies to a claim for breach of confidence).

Nevertheless, that duty has been extended beyond the physician-patient context to healthcare corporations because the "cloak of confidentiality wraps around more than the health care professional who renders . . . services." Doe v. Cmty. Health Plan–Kaiser Corp., 268 A.D.2d at 186 (reversing grant of summary judgment and finding action for breach of confidence sustainable against healthcare corporation).

B. Application

Although there is no binding precedent extending a claim for breach of confidence to a healthcare provider like Health Quest, this Court, sitting in diversity, is bound to "predict how the forum state's highest court would decide the issue." DiBella v. Hopkins, 403 F.3d 102, 111 (2d Cir. 2005). This is especially true "where sufficient precedents exist for" the federal court to

make a determination. Amerex Grp., Inc. v. Lexington Ins. Co., 678 F.3d 193, 199–200 (2d Cir. 2012).

Sufficient precedent exists here. The New York Court of Appeals has stated:

> A medical corporation may . . . be liable in tort for failing to establish adequate policies and procedures to safeguard the confidentiality of patient information or to train their employees to properly discharge their duties under those policies and procedures. Those potential claims provide the requisite incentive for medical providers to put in place appropriate safeguards to ensure protection of a patient's confidential information.

Doe v. Guthrie Clinic, Ltd., 22 N.Y.3d 480, 485 (2014). Although the Court of Appeals found no actionable breach of confidence claim, its pronouncement is sufficient for the Court to conclude New York would permit plaintiffs to pursue a breach of confidence claim in this case. See, e.g., United States v. Bell, 524 F.2d 202, 206 (2d Cir. 1975) (distinguishing "between 'obiter dictum,' which constitutes an aside or an unnecessary extension of comments, and considered or 'judicial dictum' where [a] Court, as in this case, is . . . [guiding] the future conduct of inferior courts.").

Defendant argues the Court should not recognize a duty of confidentiality here because New York courts have only recognized such a duty "in the context of communications protected by privilege, such as those between physician-patient, psychologist-patient, psychiatrist-patient, social worker-client, or attorney-client." (Def.'s Mem. at ECF 28).

Not so. New York courts have extended the duty of confidentiality beyond the physician-patient context. Doe v. Cmty. Health Plan–Kaiser Corp., 268 A.D.2d at 186–87. The "cloak of confidentiality" extends to situations when, as here, a patient must provide his or her medical information to a medical corporation that provides treatment through its healthcare providers at its facilities. See id. at 187. This extension derives from the agency relationship present when a healthcare corporation, like Health Quest, provides or facilitates medical

treatment through its agents. See id. In addition, both New York and federal statutes impose such a duty on defendant. See id.; see also 45 C.F.R. § 164.306. Accordingly, a healthcare corporation like Health Quest has a duty to keep confidential its patients' information.

This result is consistent with the holdings of other New York courts. See Jones v. Commerce Bancorp, Inc., 2006 WL 1409492, at *3 (S.D.N.Y. May 23, 2006) (finding duty of confidentiality when defendant required plaintiff to disclose personal information and "represented that it would safeguard that information.").

Plaintiffs have also alleged a breach of defendant's duty of confidentiality. When a duty of confidentiality exists, New York courts recognize it may be breached through negligent failure to safeguard confidential information. See Daly v. Metro. Life Ins. Co., 4 Misc.3d 887, 892 (Sup. Ct. N.Y. Cty. 2004) (finding victim of identity theft stated cause of action for breach of duty of confidentiality against insurance company for failing to safeguard confidential information).

Here, plaintiffs plausibly allege Health Quest negligently failed to safeguard their private information by "fail[ing] to take reasonable measures to protect the Personal Identifiable Information it collected and stored." (AC ¶ 40). Also, the Court has already determined plaintiffs plausibly allege they suffered cognizable damages sufficient to support claims sounding in tort.

Accordingly, the Court denies defendant's motion to dismiss plaintiffs' claim for breach of confidence with respect to plaintiffs Wallace, Super, Williamson, and Crispell. For the reasons discussed in Part III, supra, defendant's motion is granted with respect to plaintiffs Gyscek and Digilio.

VIII. Breach of Bailment

Defendant argues plaintiffs' claim for breach of bailment must be dismissed.

The Court disagrees.

A. Applicable Law

A Bailment is the delivery of personal property by a bailor to a bailee who holds the property for a certain purpose. *Bailment*, Black's Law Dictionary (11th ed. 2019); see Mays v. New York, N.H. & H.R. Co., 197 Misc. 1062, 1063–64 (App. Term 1st Dep't 1950). Although bailments are contractual in nature, they create a common-law duty that may be breached by negligence. See Tischler Roofing & Sheet Metal Works Co. v. Sicolo Garage, Inc., 64 Misc. 2d 825, 826 (App. Term 1st Dep't 1970).

Once a bailment has been established, to state a claim for breach of a bailment, the bailor must plead the bailee failed to "exercise care and diligence in protecting and keeping safe" the bailee's property. See Mack v. Davidson, 55 A.D.2d 1027, 1028 (4th Dep't 1977). The bailee has the burden of proof to explain the loss or destruction of the property. Herrington v. Verrilli, 151 F. Supp. 2d 449, 459 (S.D.N.Y. 2001).

Under New York law, bailments may be actual or constructive. See Herrington v. Verrilli, 151 F. Supp. 2d at 457. A constructive bailment "arises when the person having possession [of property] holds it under such circumstances that the law imposes an obligation to deliver [the property] to another." Mays v. New York, N.H. & H.R. Co., 197 Misc. at 1064. Specifically, a constructive bailment arises when a defendant takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it. See Ancile Inv. Co., Ltd. v. Archer Daniels Midland Co., 784 F. Supp. 2d 296, 307 (S.D.N.Y. 2011).

Constructive bailments do not require an express assumption of duties, and "may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner." Ancile Inv. Co., Ltd. v. Archer Daniels Midland Co., 784 F. Supp. 2d at 307.

B. Application

Plaintiffs plausibly allege a claim for breach of bailment. Plaintiffs allege they entrusted their Private Information to defendant for the purpose of obtaining medical care at one of defendant's facilities. Plaintiffs further allege defendant accepted possession of their Private Information, and that they and defendant intended and understood defendant would safeguard that information. To support their contentions, plaintiffs point to the Notice of Privacy Practices, which states Health Quest was "committed to protecting medical information about [plaintiffs]." (AC ¶ 46). Finally, plaintiffs allege defendant failed to exercise reasonable care and diligence in keeping safe their Private Information. Plaintiffs thus plausibly allege defendant acted as bailee for plaintiffs' Private Information and failed to exercise due care in doing so.

Defendant argues plaintiffs' claim should fail because intangible property, like plaintiffs' Private Information, cannot be the subject of a bailment. (Def.'s Mem. at ECF 29).

The Court disagrees.

Neither party nor the Court has identified any binding precedent addressing whether a bailment may be created for solely intangible property like the Private Information. However, the New York Court of Appeals has recognized a plaintiff may state a claim for conversion of digitally stored information such as emails and computer files. See Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d 283, 291 (2007). Given this modest extension of the common law, and that

claims for conversion and bailment historically concern similar types of property, the Court is persuaded New York's courts would extend a claim for breach of bailment to similarly intangible information. See Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d at 291 ("It is the strength of the common law to respond, albeit cautiously and intelligently, to the demands of commonsense justice in an evolving society.").

Accordingly, the motion to dismiss plaintiffs' bailment claim is denied.

IX. GBL § 349

Section 349 of New York's General Business Law prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." To assert a claim under Section 349 a "plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." Orlander v. Staples, Inc., 802 F.3d at 300.

New York courts define the term "deceptive acts and practices" objectively, as "representations or omissions, limited to those likely to mislead a reasonable consumer acting reasonably under the circumstances." Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A., 85 N.Y.2d 20, 26 (1995). GBL § 349 is not subject to the heightened pleading requirements necessary to prove fraud in other contexts. See Pelman ex rel. Pelman v. McDonald's Corp., 396 F.3d 508, 511 (2d Cir. 2005).

Plaintiffs plausibly allege a violation of GBL § 349. Defendant's statements regarding its privacy practices and data protection, in particular the Notice of Privacy Practices posted on its website, are consumer-oriented conduct. See, e.g., Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A., 85 N.Y.2d at 25 (holding plaintiffs need only "demonstrate that the acts or practices have a broader impact on consumers at large.").

Moreover, plaintiffs plausibly allege Health Quest made material misrepresentations. The Notice of Privacy Practices state Health Quest is "committed to protecting medical information," and would notify its customers of any potential data breach without any unreasonable delay. (AC ¶ 46, 158–59, 161–63). It is at least plausible that these statements would have led a reasonable consumer to believe Health Quest employed data security measures adequate to safeguard their information, and that Health Quest would promptly notify them of a data breach. See, e.g., Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 776–77 (W.D.N.Y. 2017) (finding allegations defendant would "maintain adequate data privacy and security practices" and "comply with requirements of relevant federal and state laws" plausibly alleged material misrepresentation). Plaintiffs plausibly allege defendant failed to fulfill these expectations both by failing to promptly notify them of any data breach, and by failing to implement safeguards to protect their Private Information.

As the Court concluded above, plaintiffs' allegations that they were denied the benefit of the bargain for Health Quest's services are sufficient to plausibly plead damages resulting from Health Quest's allegedly deceptive practices. See, e.g., In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d at 995–96.

Accordingly, all plaintiffs state a claim for violation of GBL § 349.

X. GBL § 899-aa

Defendant argues plaintiffs' claim under GBL § 899-aa must be dismissed because the statute does not support a private right of action.

The Court "has discretion to deem a claim abandoned when a defendant moves to dismiss that claim and the plaintiff fails to address in their opposition papers defendant's arguments for

dismissing such a claim." Estate of M.D. ex rel. DeCosmo v. New York, 241 F. Supp. 3d 413, 423 (S.D.N.Y. 2017).

Plaintiffs do not oppose defendant's argument. Accordingly, the Court deems the claim abandoned.

**CONCLUSION**

The motion to dismiss is GRANTED IN PART and DENIED IN PART. Plaintiffs' claims under GBL § 899-aa and for breach of express contract are dismissed. In addition, plaintiffs Stephen Gyscek and Nicole Digilio's claims for negligence and breach of confidence are dismissed. All other claims shall proceed.

By April 5, 2021, defendant shall file its answer to the amended complaint. (Doc. #34).

By separate Order, the Court will schedule an initial conference.

The Clerk is instructed to terminate the motion. (Doc. #42).

Dated: March 22, 2021
White Plains, NY

SO ORDERED:

Vincent L. Briccetti
United States District Judge